CLAIMS

1. Method for ensuring the integrity of at least one computer software program which can be carried out by means of at least one encryption/decryption module, the at least one computer software program being transmitted, by means of a transmitter, to a decoder which is equipped with the at least one encryption/decryption module by means of a long-distance information transmission network,
the transmitter carrying out:
a) a step (40) for encrypting information signals transmitted to the decoder,
b) a step (50) for transmitting, to the at least one encryption/decryption module of the decoder, a message containing the information required for the decoder to decrypt the information signals transmitted at step a), and
c) a step (42, 100) for transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder,
the decoder carrying out:
d) a step (74) for decrypting the information signals transmitted by the transmitter during step a) using the information provided for this purpose in the message transmitted during step b),
characterised:
- in that the transmitter inserts (at 52, 124) in the message transmitted during step b) an additional item of information which allows the at least one encryption/decryption module to verify that it has effectively received the or each computer software program transmitted at step c),
- in that the at least one encryption/decryption module verifies (at 60), based on the additional information inserted by the transmitter in the message transmitted during

step b), whether it has effectively received the or each software program transmitted during step c), and
- in that, if the or each software program has not been received, the at least one encryption/decryption module prevents step d) (at 68).

2. Method according to claim 1, characterised in that the transmitter encrypts (at 50) the message transmitted at step b), and in that the at least one encryption/decryption module decrypts the message transmitted during step b) in order to allow step d) to be carried out.

3. Method according to claim 1 or 2, characterised in that the transmitter carries out:
e) a step (44, 122) for constructing a first identifier of the or each computer software program transmitted during step c), and
f) a step (52, 124) for inserting this identifier in the message transmitted during step b),
and in that the at least one encryption/decryption module carries out:
g) a step (62, 110) for reconstructing the identifier of the or each computer software program based on the or each computer software program received,
h) a step (66, 112) for comparing the identifier reconstructed at step g) with the identifier inserted by the transmitter during step f), and
i) if the identifier reconstructed at step g) does not correspond to that inserted at step f) in the message transmitted at step b), a step (68, 108) for preventing step d),
j) if the identifier reconstructed at step g) corresponds to the identifier inserted at step f) in the message transmitted

during step b), a step (66, 112) for validating the integrity of the or each computer software program.

4. Method according to claim 3, for ensuring the integrity of a group of several computer software programs which can each be carried out by the at least one encryption/decryption module, characterised in that step e) comprises an operation (44) for constructing a single identifier for the group of several computer software programs to be transmitted during step c) based on information relating to each of the software programs of the group and in that step g) consists in carrying out the same operation as that carried out during step e) in order to reconstruct a unique identifier corresponding to that constructed during step e) if the group received by the decoder is identical to that transmitted by the transmitter.

5. Method according to claim 3 or 4, characterised in that the steps d), g), h), i) and j) are carried out by the same encryption/decryption module.

6. Method according to claim 3 or 4, characterised in that a first autonomous encryption/decryption module carries out only steps d), h), i) and j), and in that a second autonomous encryption/decryption module which is independent from the first encryption/decryption module and which is fixedly joined to the decoder carries out at least step g).

7. Method according to claim 6, characterised in that the transmitter further carries out:
k) a second step (120) for constructing a second identifier of the or each computer software program transmitted during step c), this second identifier being transmitted together

with the or each corresponding software program during step c), and

- in that step g) which is carried out by the second encryption/decryption module comprises:

- an operation (102) for reconstructing the second identifier which is transmitted together with the or each software program,

- only if the second reconstructed identifier corresponds to that transmitted together with the or each software program during step c), an operation (110) for reconstructing the first identifier inserted in the message transmitted during step b) and for transmitting this first reconstructed identifier to the first encryption/decryption module so that the first encryption/decryption module can carry out step h).

8. Method according to claim 7, characterised in that the first and the second identifiers are obtained from the same identifier of the or each computer software program by encrypting the same identifier using a different first and second encryption key, respectively.

9. Method according to any one of claims 2 to 8, characterised in that the at least one encryption/decryption module carries out the at least one computer software program each time the integrity thereof is validated during step j).

10. Information recording medium (12) comprising instructions for carrying out a method according to any one of the preceding claims, when the instructions are carried out by the transmitter (4).

11. Information recording medium (22, 88) comprising instructions for carrying out a method according to any one

of claims 1 to 9, when the instructions are to be carried out by the at least one encryption/decryption module.

12. System for ensuring the integrity of at least one computer software program which can be carried out by at least one encryption/decryption module (16, 84), the system comprising a transmitter (4) for transmitting the at least one computer software program via a long-distance information transmission network (8), and a decoder (6, 82) which is equipped with the at least one encryption/decryption module (16, 84),
the transmitter (4) being capable of:
- encrypting information signals transmitted to the or each decoder,
- transmitting to the at least one encryption/decryption module of the decoder a message containing the information required for the decoder to decrypt the information signals transmitted, and
- transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder,
- the decoder (6, 82) being capable of decrypting the information signals transmitted by the transmitter using the information which is provided for this purpose and which is contained in the message transmitted by the transmitter,
characterised:
- in that the transmitter (4) is capable of inserting in the message an additional item of information which allows the at least one encryption/decryption module (46, 84) to verify that it has received the or each computer software program transmitted,
- in that the at least one encryption/decryption module (16, 84) is capable of verifying, based on the additional information inserted by the transmitter in the message,

whether it has effectively received the or each software program transmitted by the transmitter, and
- in that, if the or each software program has not been received, the at least one encryption/decryption module (16, 84) is capable of preventing the decryption of the information signals transmitted.

13. System according to claim 12, characterised in that the or each decoder (6) is equipped with a single removable encryption/decryption module.

14. System according to claim 12, characterised in that the or each decoder (82) is equipped with at least two autonomous encryption/decryption modules which are independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder.

15. Transmitter (4) which is suitable for carrying out a method according to any one of claims 1 to 9, this transmitter (4) being capable of:
- encrypting information signals transmitted to the or each decoder,
- transmitting to the at least one encryption/decryption module of the decoder a message containing the information required for the decoder to decrypt the information signals transmitted, and
- transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder, characterised:
- in that the transmitter (4) is capable of inserting in the message an additional item of information which allows the at least one encryption/decryption module (46, 84) to verify

that it has received the or each computer software program transmitted.

16. Decoder (6, 82) which is suitable for carrying out a method according to any one of claims 1 to 9, this decoder (6, 82) being capable of decrypting the information signals transmitted by the transmitter using the information which is provided for this purpose and which is contained in the message transmitted by the transmitter, and being equipped with the at least one encryption/decryption module (16, 84); characterised:
- in that the at least one encryption/decryption module (16, 84) is capable of verifying, based on the additional information inserted by the transmitter in the message, whether it has effectively received the or each software program transmitted by the transmitter, and
- in that, if the or each software program has not been received, the at least one encryption/decryption module (16, 84) is capable of preventing the decryption of the information signals transmitted.

17. Decoder (6, 82) according to claim 16, characterised in that it is equipped with a single removable encryption/decryption module.

18. Decoder (6, 82) according to claim 16, characterised in that it is equipped with at least two autonomous encryption/decryption modules which are independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder.